



Identity Theft: Reducing the Risk of Fraud


Consumer Protection and Antitrust
Bureau

NH Attorney General's Office

33 Capitol Street
Concord, NH 03301
(603) 271-3641
1-888-468-4454

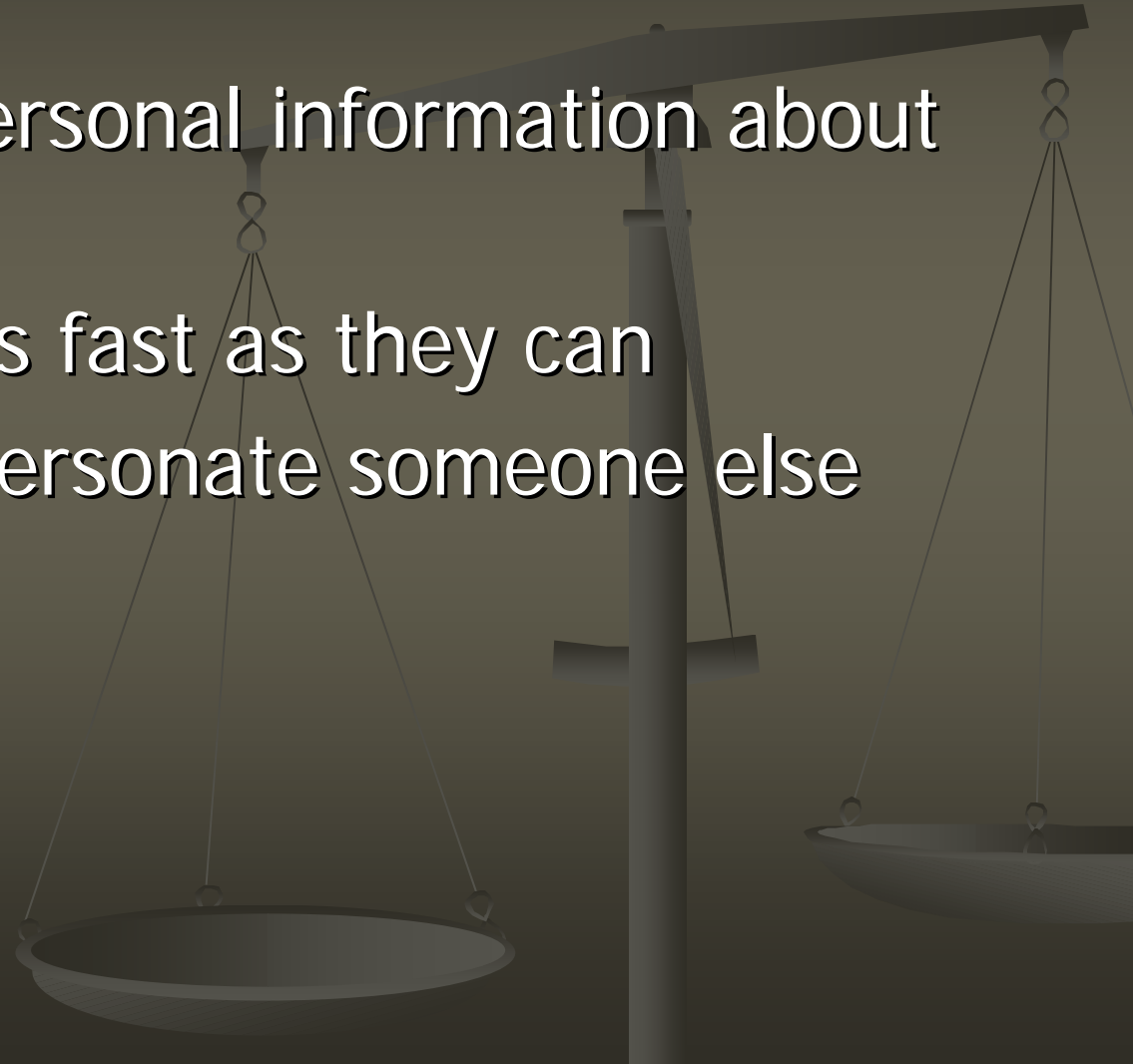
<http://www.nh.gov/consumer>

Agenda

- Identity Theft – America's fastest growing type of robbery
 - Consumers lost \$50 billion last year
 - Estimated 9.9 million victims in America
 - What is it?
 - What information is stolen?
 - Types of identity theft
 - How they obtain your information
 - How you can protect yourself
 - What to do if you're a victim
- 

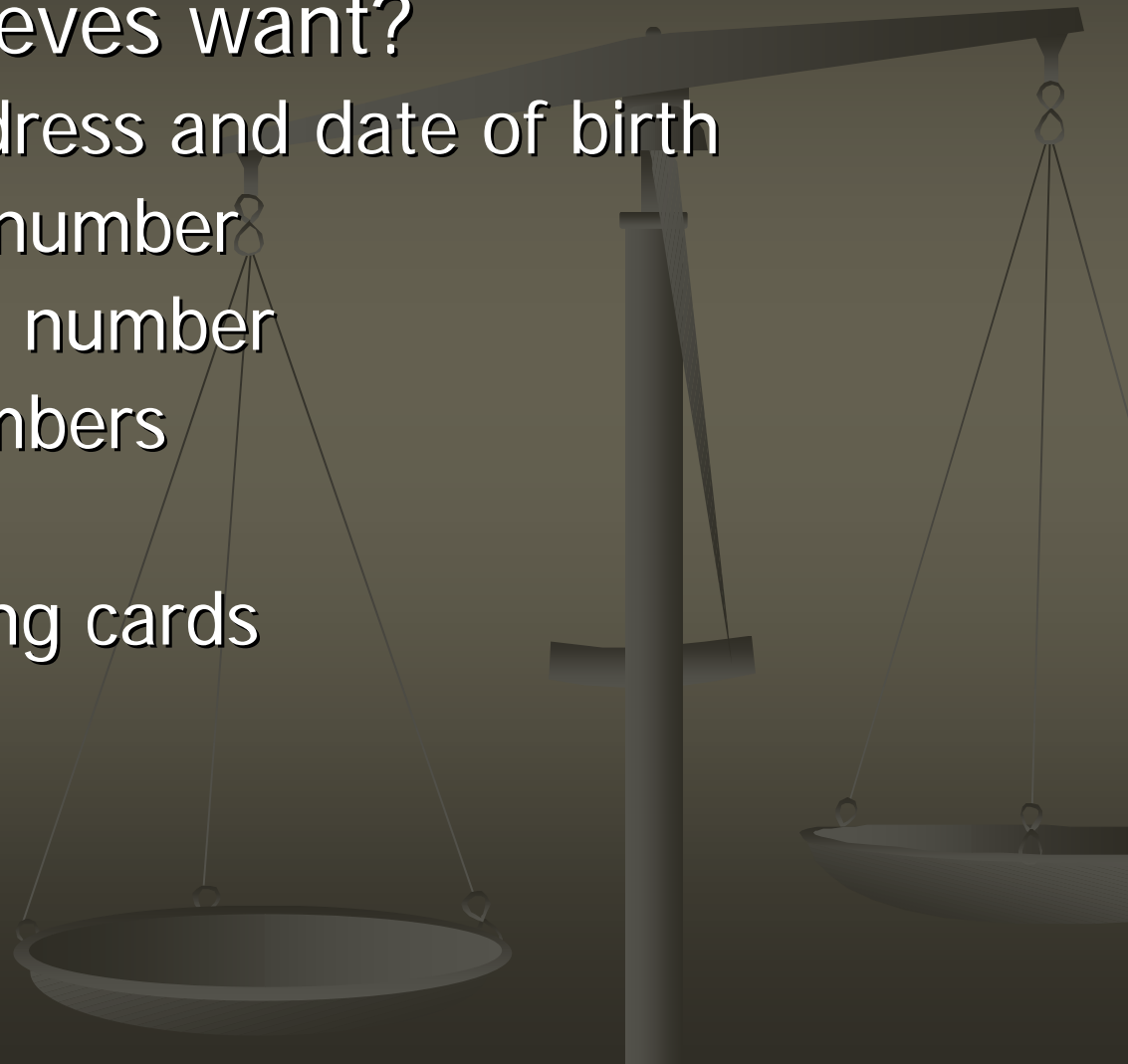
What is Identity Theft

- Thieves steal personal information about you
- Spend money as fast as they can
- Move on to impersonate someone else



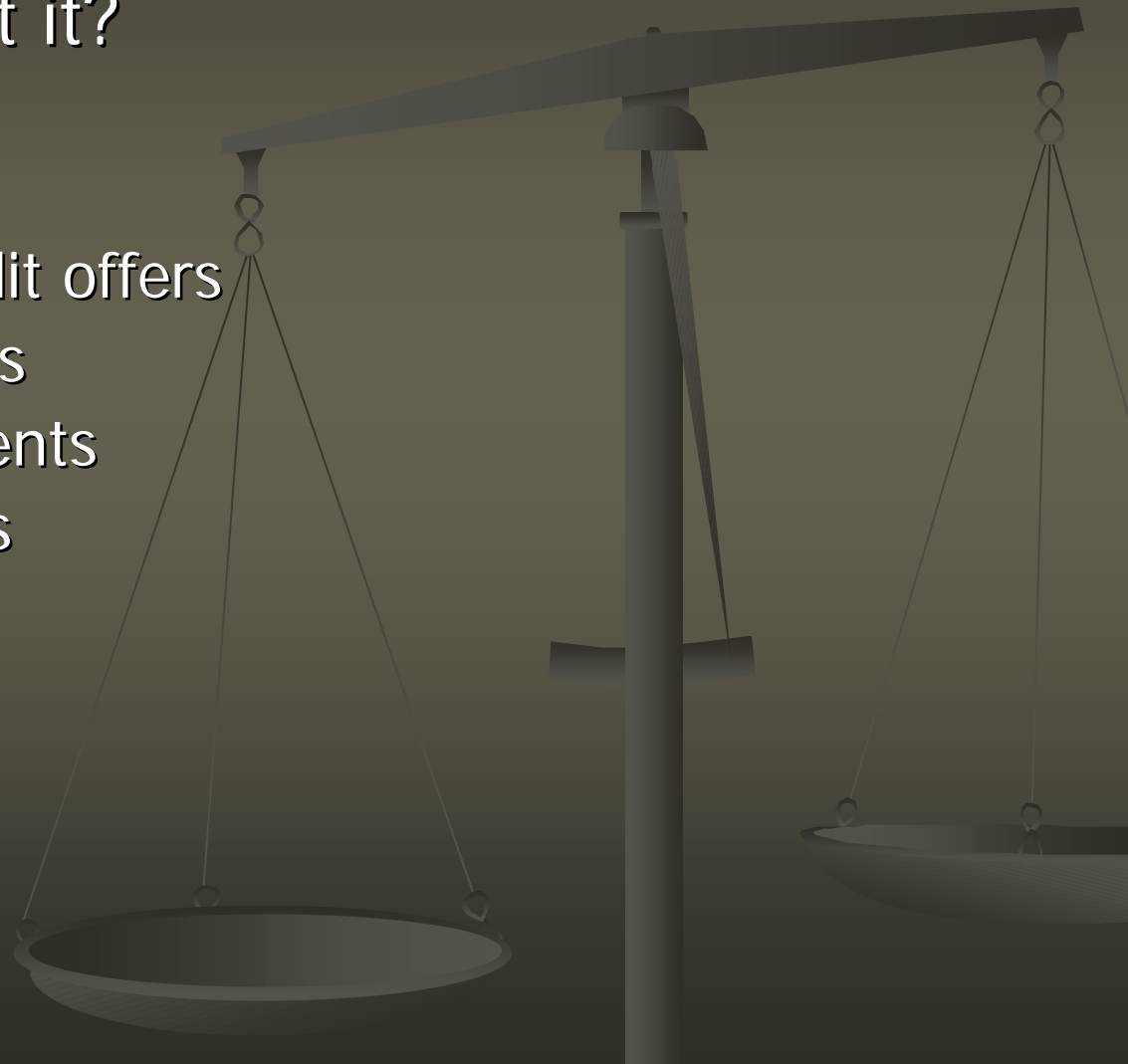
Personal Information

- What do the thieves want?
 - Your name, address and date of birth
 - Social Security number
 - Driver's License number
 - Credit Card numbers
 - ATM cards
 - Telephone calling cards



Personal Information

- Where do they get it?
 - Credit cards
 - Driver's Licenses
 - Pre-approved credit offers
 - Investment reports
 - Insurance statements
 - Benefit documents
 - Tax information
 - Personal checks



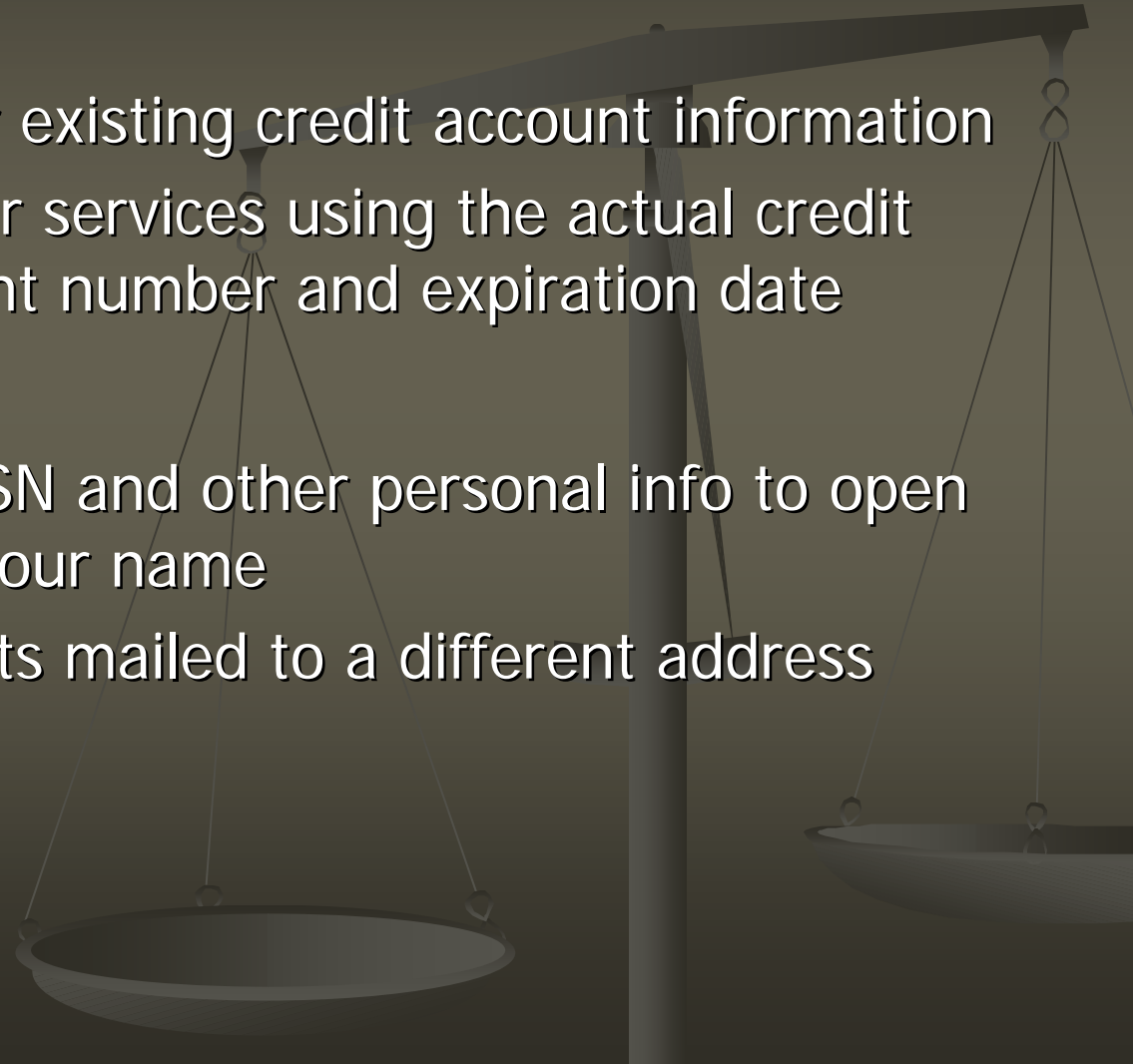
Types of Identity Theft

■ Account Takeover

- Thief obtains your existing credit account information
- Purchases items or services using the actual credit card or the account number and expiration date

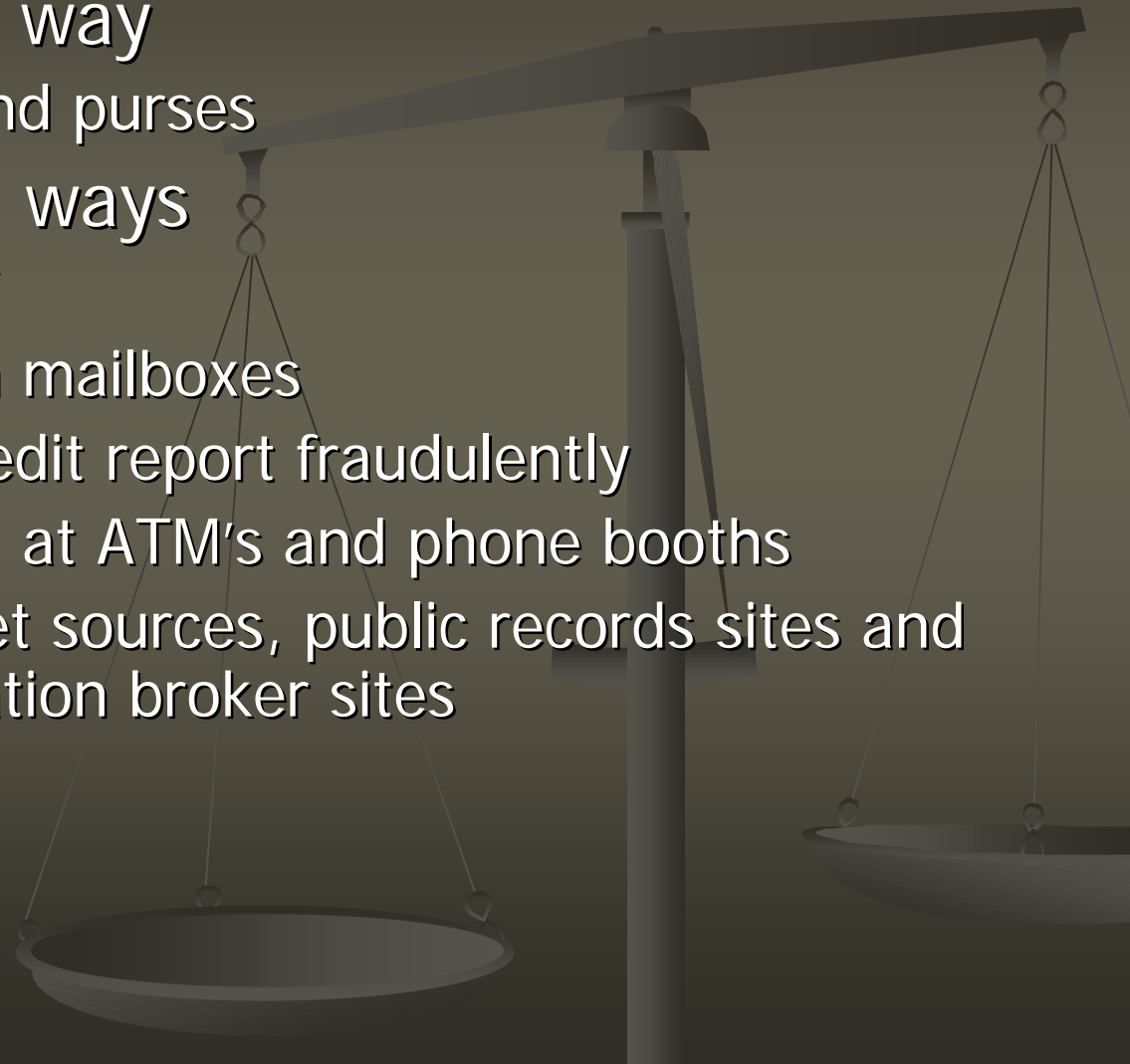
■ Application Fraud

- Thief uses your SSN and other personal info to open new accounts in your name
- Monthly statements mailed to a different address



How Do They Get Your Identity?

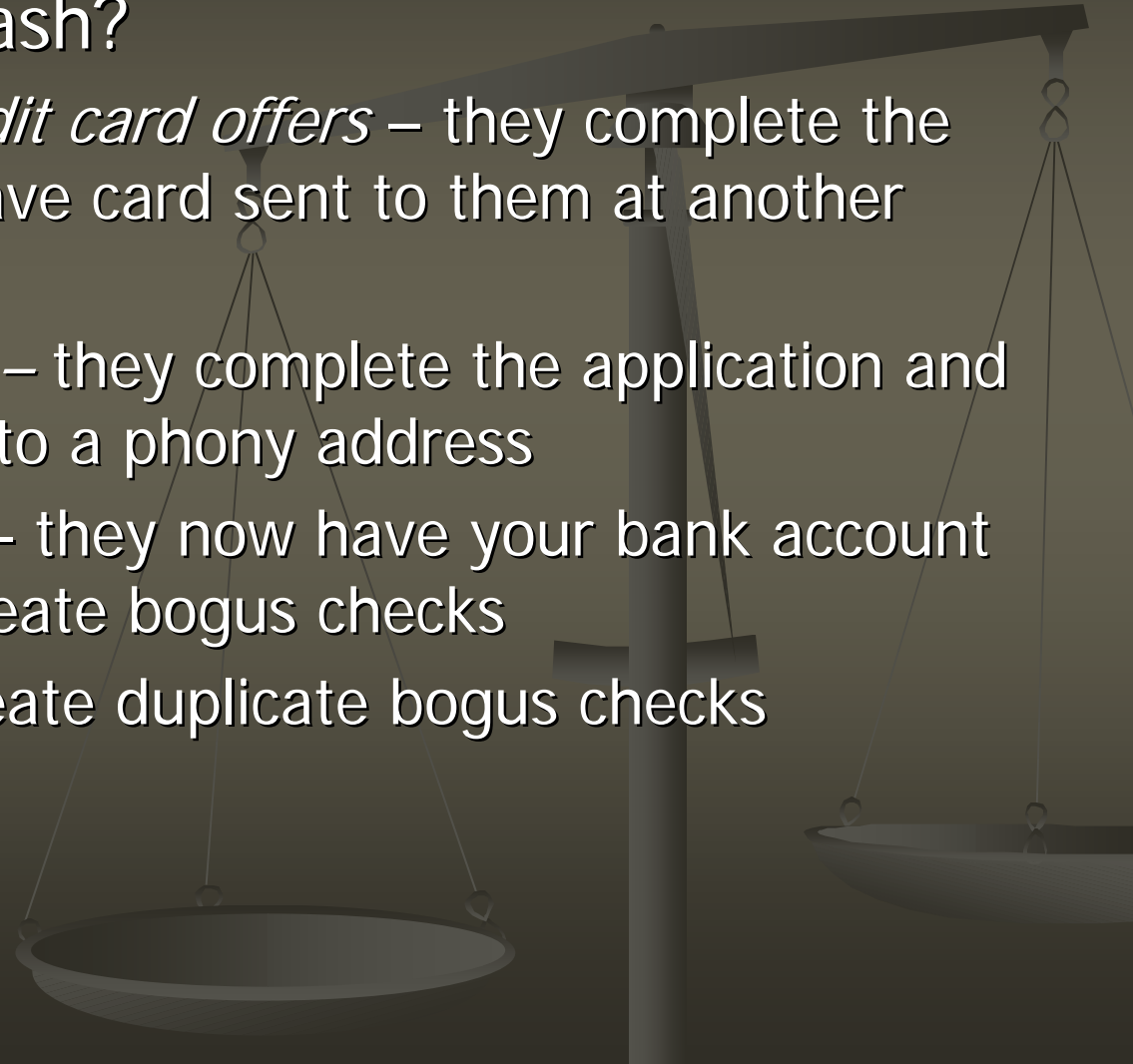
- The old-fashioned way
 - Stealing wallets and purses
- New sophisticated ways
 - “Dumpster diving”
 - Stealing mail from mailboxes
 - Accessing your credit report fraudulently
 - “Shoulder surfing” at ATM’s and phone booths
 - Looking at Internet sources, public records sites and fee-based information broker sites



Dumpster Diving: Trash or Treasure

■ What's in Your Trash?

- *Pre-approved credit card offers* – they complete the application and have card sent to them at another address
- *Loan applications* – they complete the application and have money sent to a phony address
- *Bank statements* – they now have your bank account numbers. They create bogus checks
- *Checks* – They create duplicate bogus checks

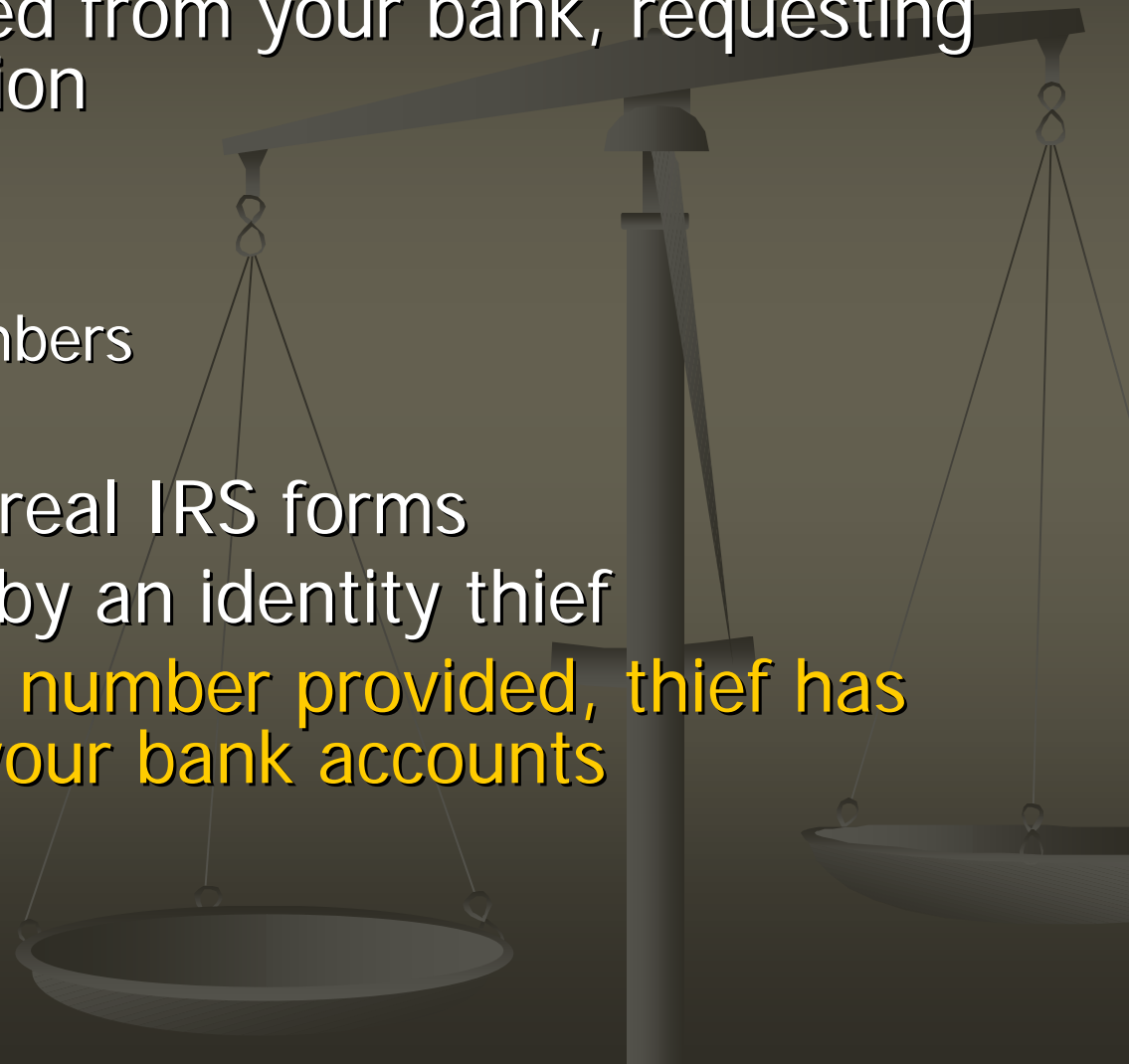


ATM Fraud Scheme

- Plastic strip placed into card insert
 - Machine cannot read the card
 - Machine continuously asks for PIN
- Thief nearby watches PIN being entered over and over
- Victim thinks ATM is broken and has the card
- Thief removes card and enters PIN

IRS Tax Form Scam

- “IRS form” received from your bank, requesting sensitive information
 - SSN
 - DOB
 - Bank account numbers
 - PIN numbers
- Form is similar to real IRS forms
- Created and sent by an identity thief
- Once faxed to the number provided, thief has info to clean out your bank accounts



Dear Customer,

We are currently updating our resident, non-resident alien and citizens' records. This is to enable us to detect persons exempted from the United States reporting and withholding tax on interest paid to you on your bank account and other financial dealings. To adequately protect such exemptions from paying tax on statutorily, we are required to update our records to enable you recertify your exemption status. To complete this exercise in time, you are required to complete the attached Form W-9095 and return same to us as soon as possible through the Fax number 1-914-470-9245.

United States citizens or resident aliens should also fill the form, indicating "U.S. Citizen/Resident" on the form and return same to us. We will on receipt, re-classify such category of customers. In completing the attached form, you are advised to follow the steps below:

- i) If you are a non-resident alien, indicate the name of your country to support your non-resident status.
- ii) U.S. Citizens and other resident aliens must indicate their permanent residential address in the U. S. This is to enable us mail further documents regarding their status.
- iii) If any signatory/ies to the account have acquired U.S. resident status after the opening of the account, please indicate same in the form.
- iv) In case of joint signatories, all such persons or holders must sign and date the form separately and fax same to the fax number indicated above.

All completed form W-9095 should be returned to us within Seven (7) days of receipt of this letter to help us update your records immediately. Please remember that if your account or financial dealings are not recertified early enough, it will be subject to U.S. reporting and withholding tax. If this is applied, we are required to withhold 31 of all interest paid to you. We appreciate your timely co-operation to help us protect your exemption status and accurately update our records.

Yours sincerely,

Monique Meeuws

Form **W-9095**(Rev. July 2001)
Department of the Treasury
Internal Revenue Service**Application Form For Certificate Status/
Ownership For Withholding Tax**
(Fax this Form to 1-814-470-8245)For Official Use Only
EPIN: ETIN:

OMB Number 1545-0047

Please check the box(es) that apply to this application:

☐ New☐ Reapply☐ Revised

EPIN: _____

☐ On-line Filing (check only if you will process income tax return information for taxpayers who are preparing their returns at home, via an On-line Internet site, or fax mail (see fax mail number below))

Revision Reason: _____

☐ Fax mail number in the foreign country if applicable.

Type or print name (first, middle, last)

☐ Tax Payer Identification Number (EIN) ☐ Social Security Number (SSN)
(State as applicable)Title: ☐ Mr. ☐ Mrs. ☐ OthersSex ☐ Male ☐ Female

U.S. Citizenship?

☐ Yes ☐ No☐ Legal resident alien

Date of Birth: Month _____ Day _____ Year _____

Place of Birth: _____

Marital Status: ☐ Married ☐ Single ☐ Divorce ☐ Widowed

Spouses Name (if any): _____

Father's Name /

Mother's Maiden Name /

Passport No. (Indicate Place and Date of Issue / Expiration): _____

Country of Permanent Residence (Address in full, Not P.O.Box): _____

Branch (Address in full, including Telephone numbers): _____

Account Name and Date it Was Opened: _____

PIN Number (if any): _____

Password or Code (if any): _____

Index Number (if any): _____

Date and Amount of last deposit _____

Account Officer (Full name & Rank if any) _____

State Other Accounts (if any): _____

Day Time Phone / Fax No. _____

Where did you work in the last 12 months? _____

When did each employment begin and end? _____

Was any part of these employments carried out in the U.S.?

☐ YES☐ NO

Do you intend to stay in the US for 6 to 12 months period?

☐ YES☐ NO

How often do you come to the US and when did you arrived last? _____

Are your spouse and children living in your country of residence?

☐ YES☐ NO

Are your parents and relations living in your country of residence?

☐ YES☐ NO**CERTIFICATION**

Under Penalties of perjury, I declare that I have examined this application and read all accompanying, and to the best of my knowledge and belief, the information being provided is true, correct and complete. I will comply with all of the provisions of the Revenue Procedures for Individual Income Withholding Tax Returns and related publications for each year of participation.

SIGNATURES

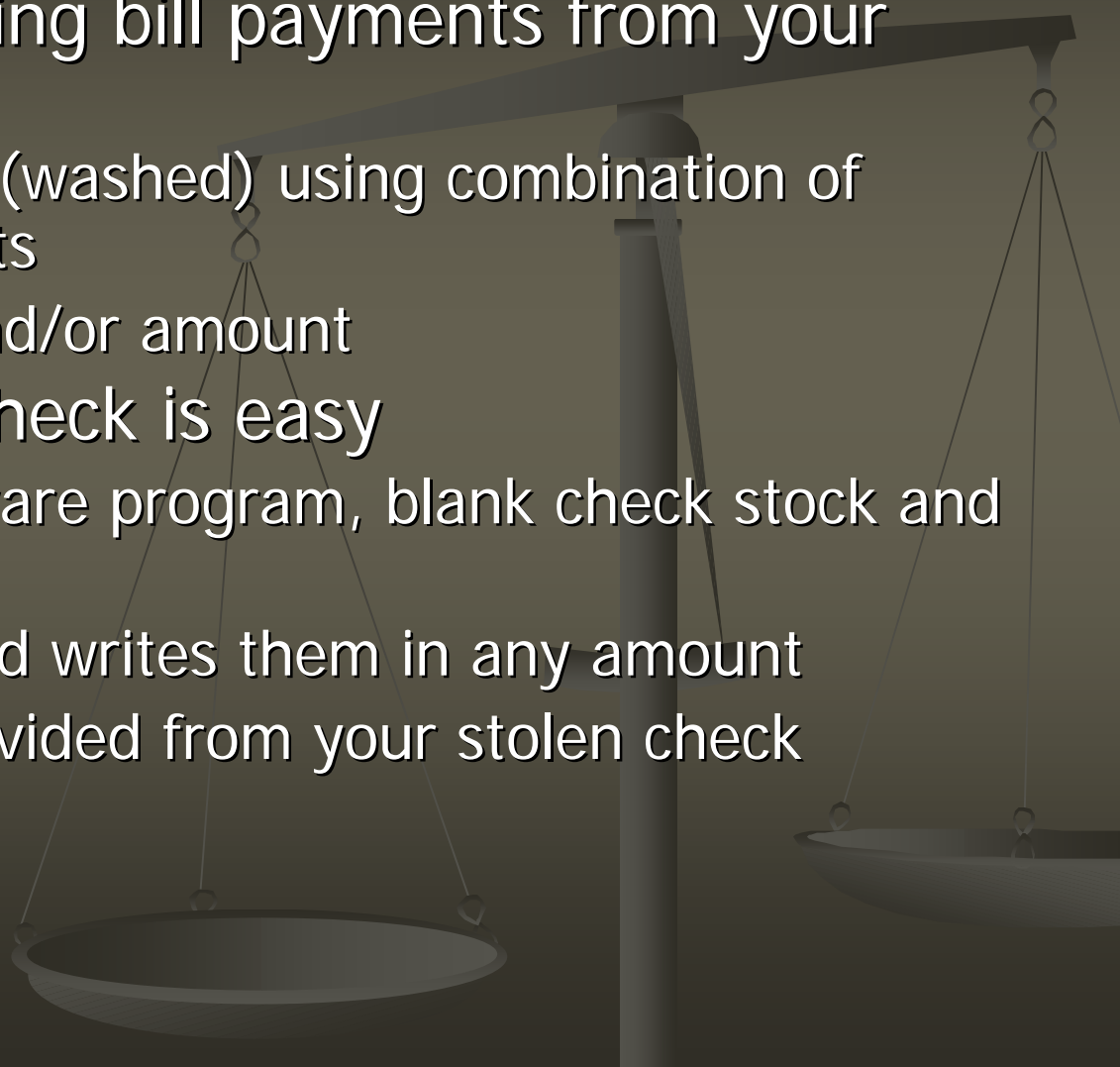
| | | | | |
|-----------|------|-------------|---------------|------|
| Signature | Name | Nationality | Date of Birth | Date |
| Signature | Name | Nationality | Date of Birth | Date |
| Signature | Name | Nationality | Date of Birth | Date |

Department Store Scam

- Purchase made using a credit card
- Phone next to register rings
- Caller is “store security” – says you are a suspect in a credit card fraud
 - Needs clerk to verify credit card information
 - May ask clerk to get address and SSN
- Call came from thief on a cell phone watching nearby

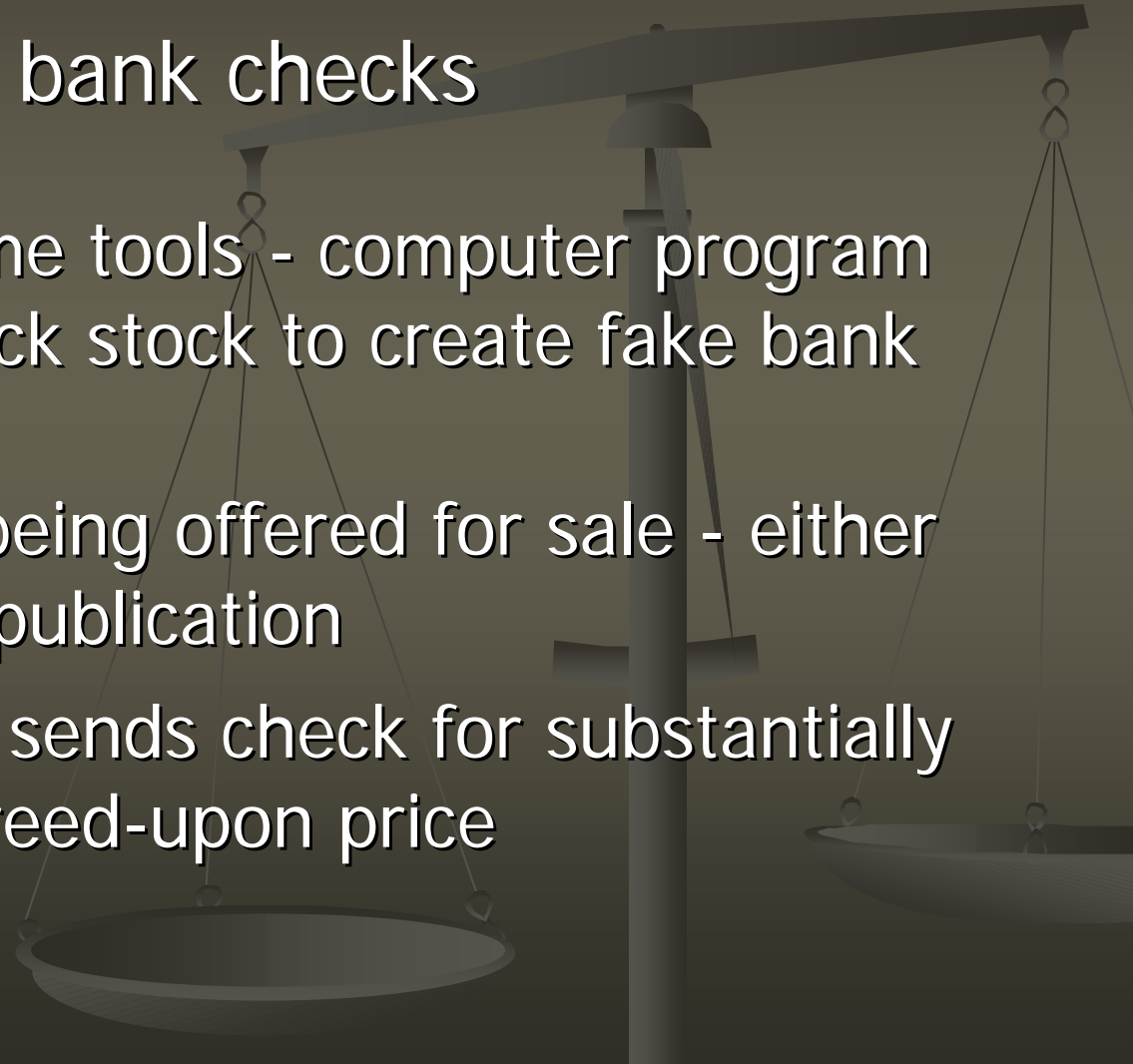
Check Washing/Counterfeit Checks

- Thief steals outgoing bill payments from your mailbox
 - Check is changed (washed) using combination of household products
 - Changes payee and/or amount
- Counterfeiting a check is easy
 - Thief uses a software program, blank check stock and a printer
 - Creates checks and writes them in any amount
 - Information is provided from your stolen check

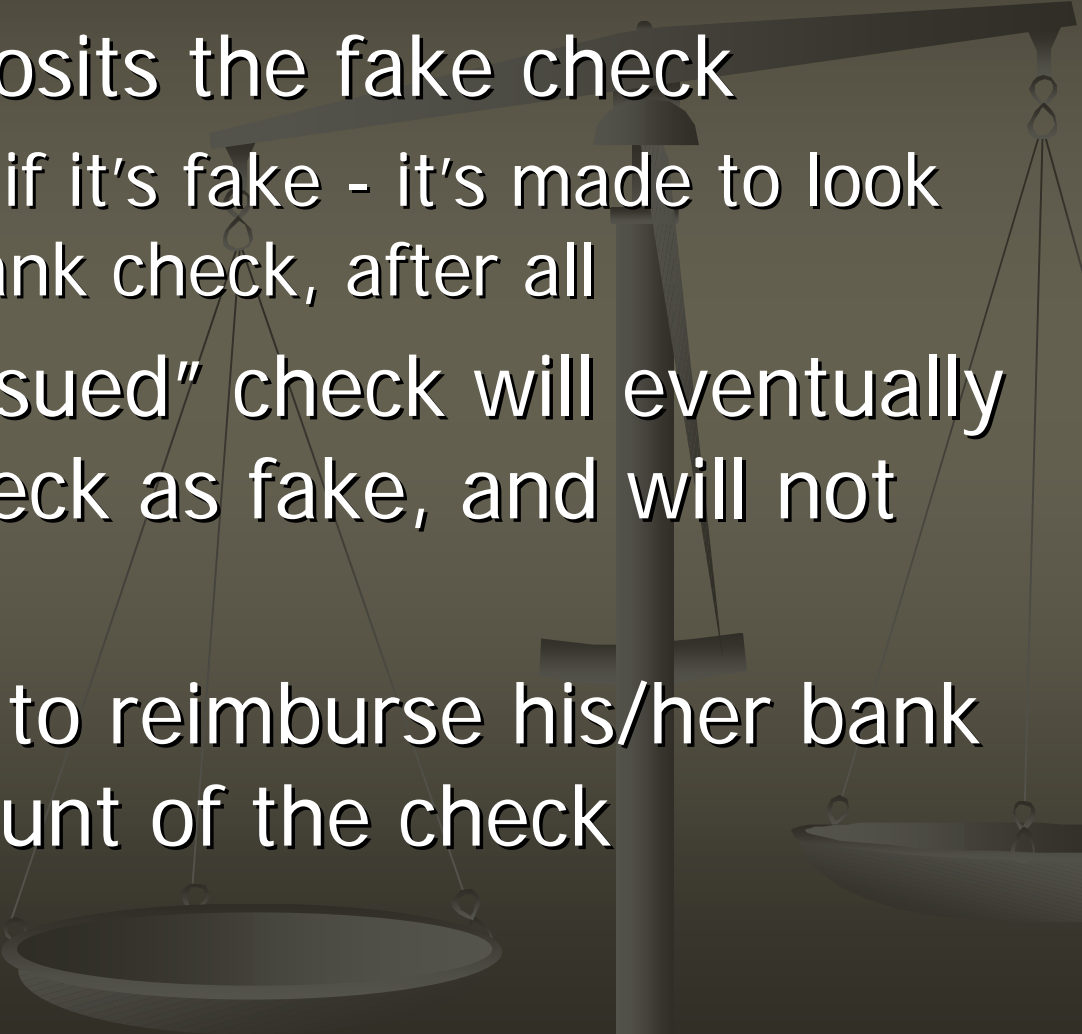


Counterfeit Checks

- Counterfeiting bank checks
 - Thief uses same tools - computer program and blank check stock to create fake bank checks
 - Locates item being offered for sale - either online or in a publication
 - Offers to buy, sends check for substantially more than agreed-upon price



Counterfeit Checks

- Consumer deposits the fake check
 - Bank can't tell if it's fake - it's made to look like another bank check, after all
 - Bank which "issued" check will eventually identify the check as fake, and will not pay
 - Consumer has to reimburse his/her bank the entire amount of the check
- 

A Counterfeit Check

THIS DOCUMENT HAS A COLORED BACKGROUND AND MICROPRINTING. THE REVERSE SIDE INCLUDES AN ARTIFICIAL WATERMARK.

 **Farmers National Bank**
Member FDIC

OFFICIAL CHECK

049229

EC-1013433

DATE: **OCTOBER 06, 2005**

PAY 

TO THE ORDER OF: **THREE THOUSAND EIGHT HUNDRED FORTY FIVE AND 00/100 US DOLLARS** **\$***3,845.00*****

 AUTHORIZED SIGNATURE


Issued by Integrated Payment Inc., Englewood Colorado To Farmers National Bank
For inquiries regarding this instrument, Phone (604) 906 1800

REMITTER:
Venture Communication Ltd

⑈049229⑈ ⑆043310139⑆ 2900010

ENDORSE HERE:

DO NOT WRITE, STAMP OR SIGN BELOW THIS LINE
RESERVED FOR FINANCIAL INSTITUTION USE

 The security features listed below, as well as those not listed, exceed industry guidelines.

Security Features:

- Micro Print Burster line
- Emboss protection
- Security Surgen

Results of document attention:

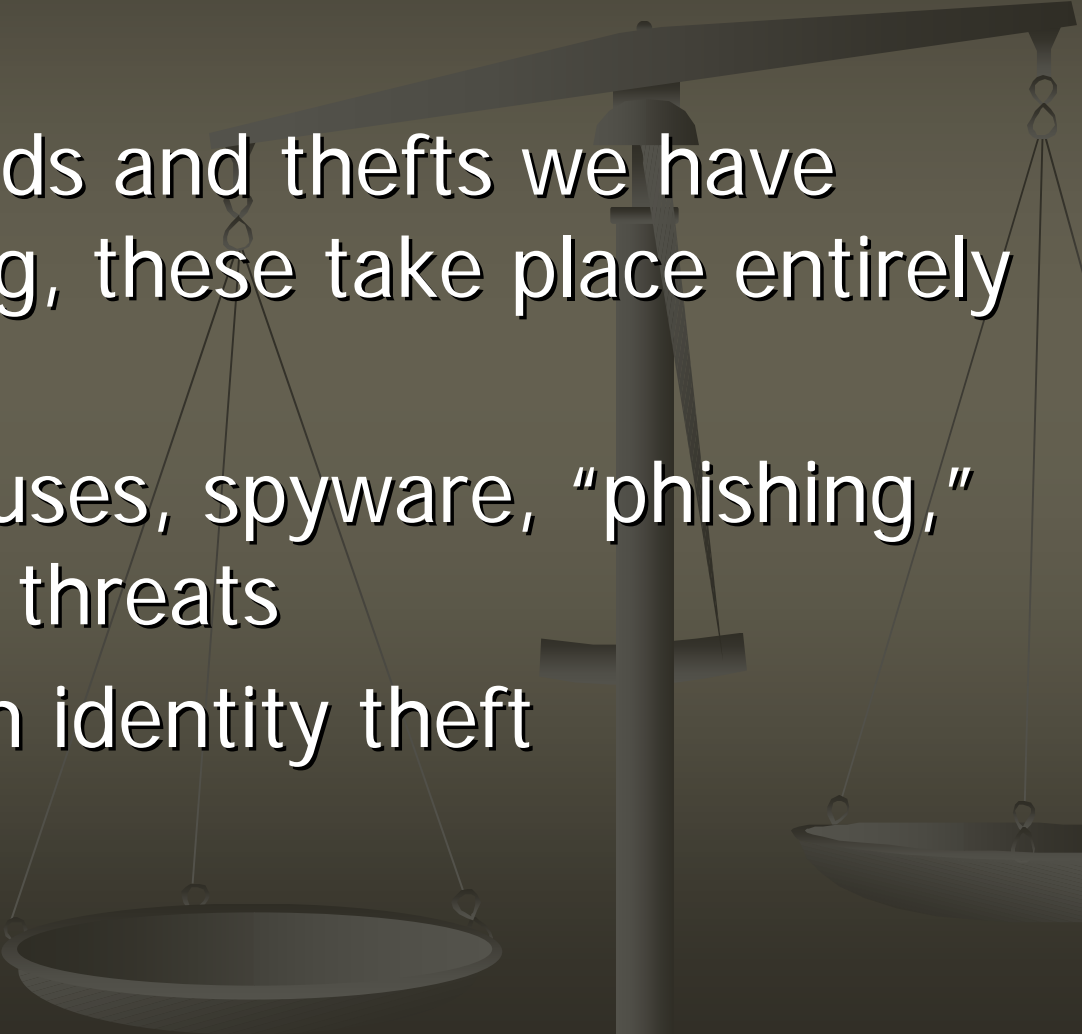
- Serial type in center and at feet
- as dotted line with photograph
- White marks above water stained
- Absence of Original Document
- Yellowish on back of check

FEDERAL RESERVE BOARD OF GOVERNORS REG. CC

Skimming Scam

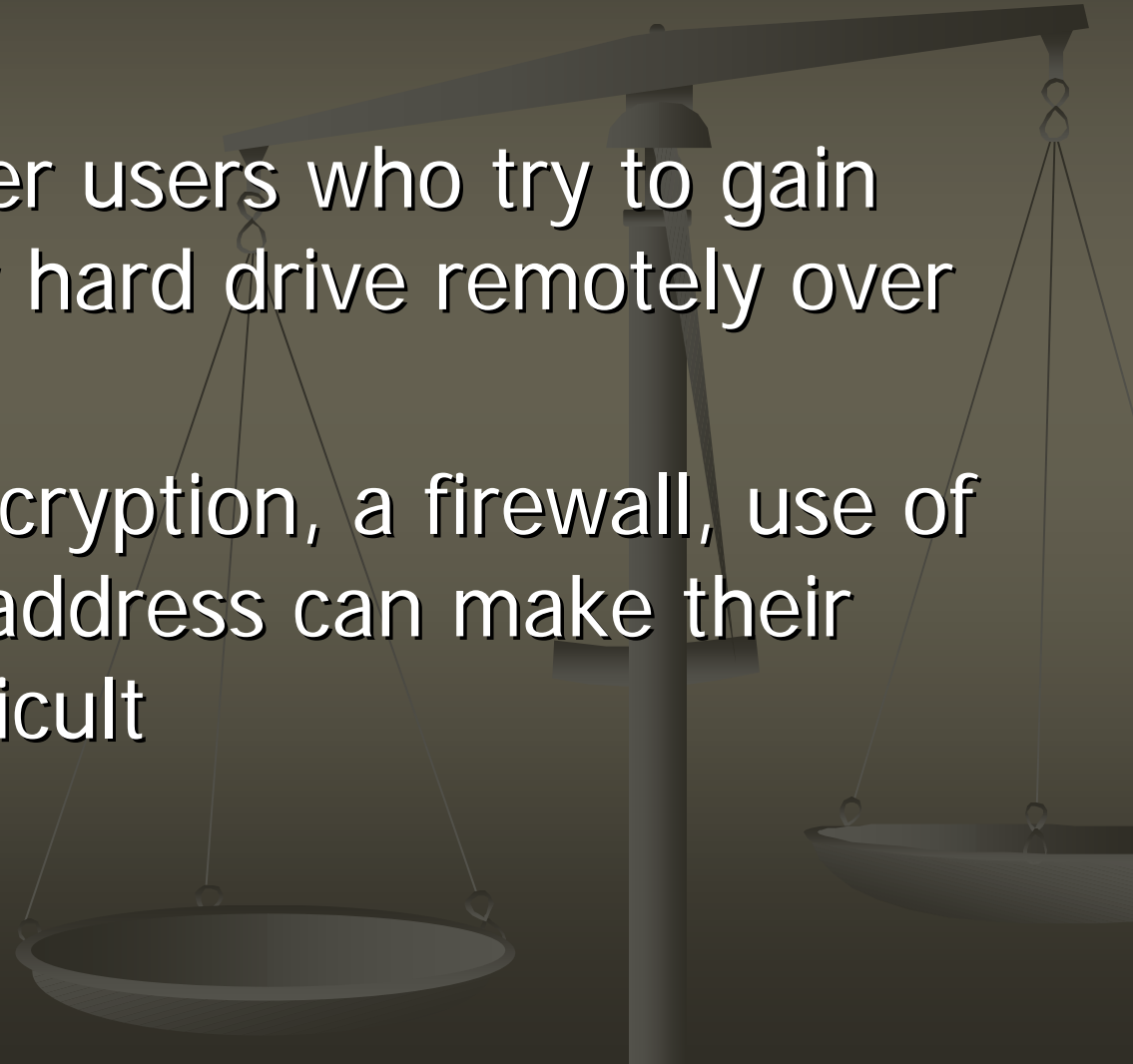
- Waiter in a restaurant takes your credit or debit card at the end of the meal
 - Uses a small hand-held electronic device (called a "skimmer") to swipe your card
 - Only takes a second
 - Your card information is stored in the skimmer
- Thief makes counterfeit card, or makes purchases over the phone or Internet

On-Line Fraud-ID Theft

- Unlike the frauds and thefts we have been discussing, these take place entirely via computer
 - “Crackers,” viruses, spyware, “phishing,” “pharming” are threats
 - All can result in identity theft
- 

“Crackers”

- Other computer users who try to gain access to your hard drive remotely over the internet
- Passwords, encryption, a firewall, use of a dynamic IP address can make their lives more difficult



Viruses and Worms

- Malicious programs that are installed without your knowledge or permission
- May be part of or enclosed in an email
 - Once installed, may replicate and propagate themselves using your computer
- Perform unwanted acts - affect stored data, may record keystrokes and “phone home” or otherwise steal sensitive data

Spyware

- ❁ A program which records your activities on your computer and “phones home.”
- ❁ May be relatively benign, or may become a threat by collecting and transmitting sensitive data
- ❁ Sometimes the spying is disclosed, often it is not. Read the EULA.

“Phishing” Scam

- You get an email that looks like it comes from your bank, credit card company, etc.
- Asking you to “update their records”
 - May be due to potential fraud, other reasons
- Provides a hyperlink to a web page where you enter your personal information
- The link takes you to a thief’s website that is disguised to look like the company’s.

“Phishing” Email

From: CitiBank [<mailto:supprefnum09624867007@citibank.com>]
Sent: Tuesday, September 14, 2004 12:04 AM
To: Rienzo, David
Subject: CitiBank AAlert - Unauthorized Login Attempts [Tue, 14 Sep 2004 07:56:17 +0400]



Dear CitiBank customer,

Recently there have been a large number of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details.

This process is mandatory, and if not completed within the nearest time your account may be subject to temporary suspension.

To securely confirm your Citibank account details please go to:

https://web.da-us.citibank.com/signin/scripts/login/user_setup.jsp

Thank you for your prompt attention to this matter and thank you for using CitiBank!

Citi® Identity Theft Solutions

Do not reply to this email as it is an unmonitored alias

A member of citigroup

Copyright © 2004 Citicorp <<https://web.da-us.citibank.com/>

[signin/scripts/login/user_setup.jsp](https://web.da-us.citibank.com/signin/scripts/login/user_setup.jsp)> <https://web.da-us.citibank.com/signin/scripts/login/user_setup.jsp>

“Phishing” Email

Received: from 199.192.4.2 ([211.238.168.26]) by NHAGEX1.doj.state.nh.us with Microsoft SMTPSVC(5.0.2195.6713);
Mon, 11 Oct 2004 05:10:27 -0400
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
FCC: mailbox://supprefnum3@suntrust.com/Sent
X-Identity-Key: id1
Date: Mon, 11 Oct 2004 05:02:16 -0500
From: SunTrust bank <supprefnum3@suntrust.com>
X-Mozilla-Draft-Info: interna!draft; vcard=0; receipt=0; uuencode=0
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.4) Gecko/20030624 Netscape/7.1 (ax)
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: David.Rienzo@doj.nh.gov
Subject: Customer service: your account in SunTrust Bank
Content-Type: multipart/related;
boundary="-----010905020308080507080007"
Return-Path: supprefnum3@suntrust.com
Message-ID: <NHAGEX1rB0Xn2Pi1Y7P00000265@NHAGEX1.doj.state.nh.us>
X-OriginalArrivalTime: 11 Oct 2004 09:10:28.0528 (UTC) FILETIME=[26CC6B00:01C4AF72]

From: SunTrust bank
<supprefnum3@suntrust.
com

“Phishing” Email

Please enter a domain address to look up its "whois" information

(ex. 10.0.2.1 or www.domain.com)

Please enter or select a whois server to search

Whois has started ...

% [whois.apnic.net node-1]
% Whois data copyright terms <http://www.apnic.net/db/dbcopyright.html>

inetnum: 211.232.0.0 – 211.255.255.255
netname: KRNIC-KR
descr: KRNIC
descr: Korea Network Information Center
country: KR
admin-c: HM127-AP
tech-c: HM127-AP
remarks: *****
remarks: KRNIC is the National Internet Registry
remarks: in Korea under APNIC. If you would like to
remarks: find assignment information in detail
remarks: please refer to the KRNIC Whois DB
remarks: <http://whois.nic.or.kr/english/index.html>
remarks: *****
mnt-by: APNIC-HM
mnt-lower: MNT-KRNIC-AP
changed: hostmaster@apnic.net 20000908
changed: hostmaster@apnic.net 20010627
status: ALLOCATED PORTABLE
source: APNIC

person: Host Master
address: 11F, KTF B/D, 1321-11, Seocho2-Dong, Seocho-Gu,
address: Seoul, Korea, 137-857
country: KR
phone: +82-2-2186-4500
fax-no: +82-2-2186-4496



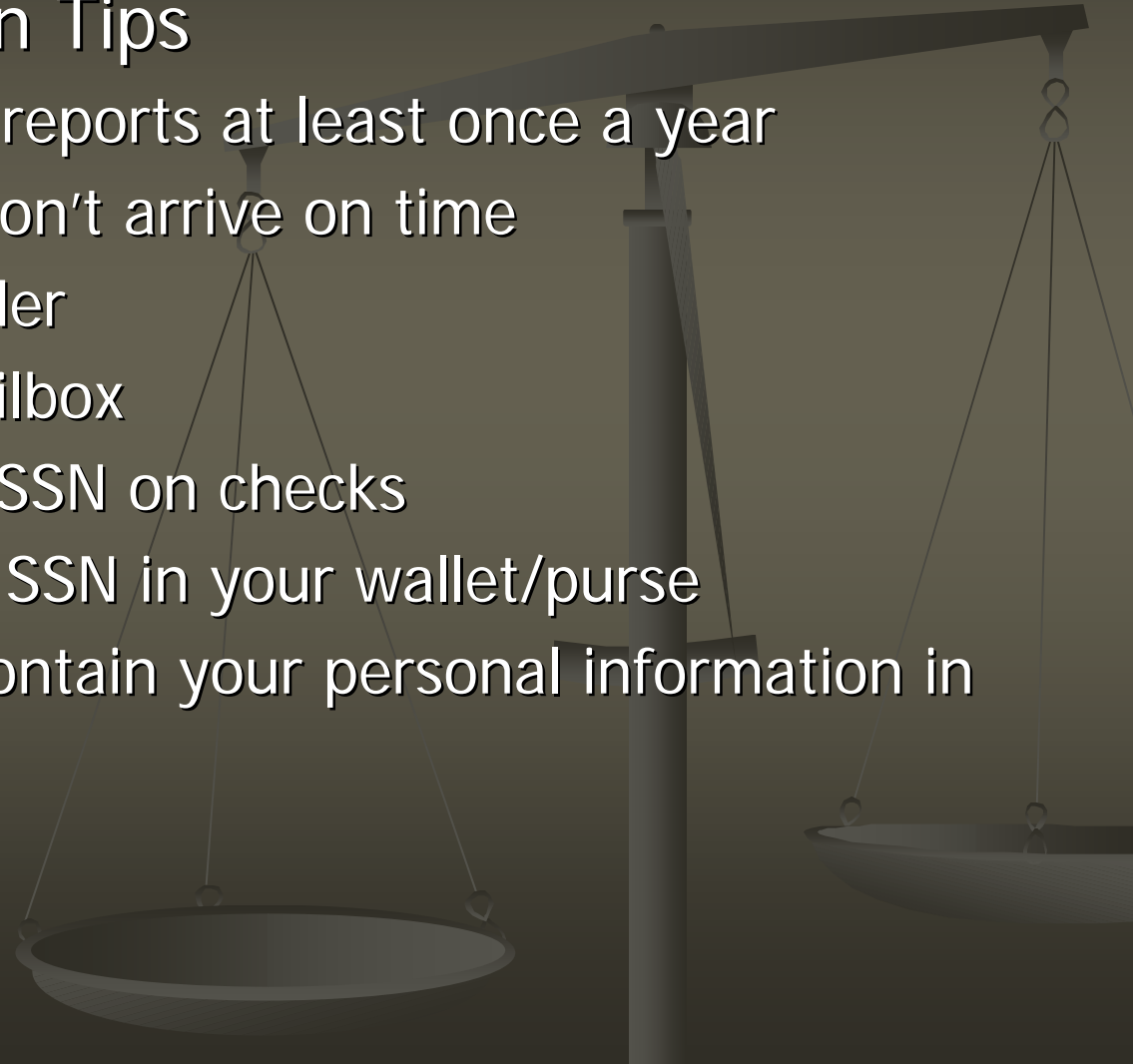
Pharming Scam

- More sophisticated than phishing
- Thief creates website that looks like a legitimate business's website
- Thief then hacks either the legitimate website or the DNS server to redirect the business's customers to his site
- Hard for thief to do, but also extremely hard for consumer to detect

How You Can Protect Yourself

■ General Prevention Tips

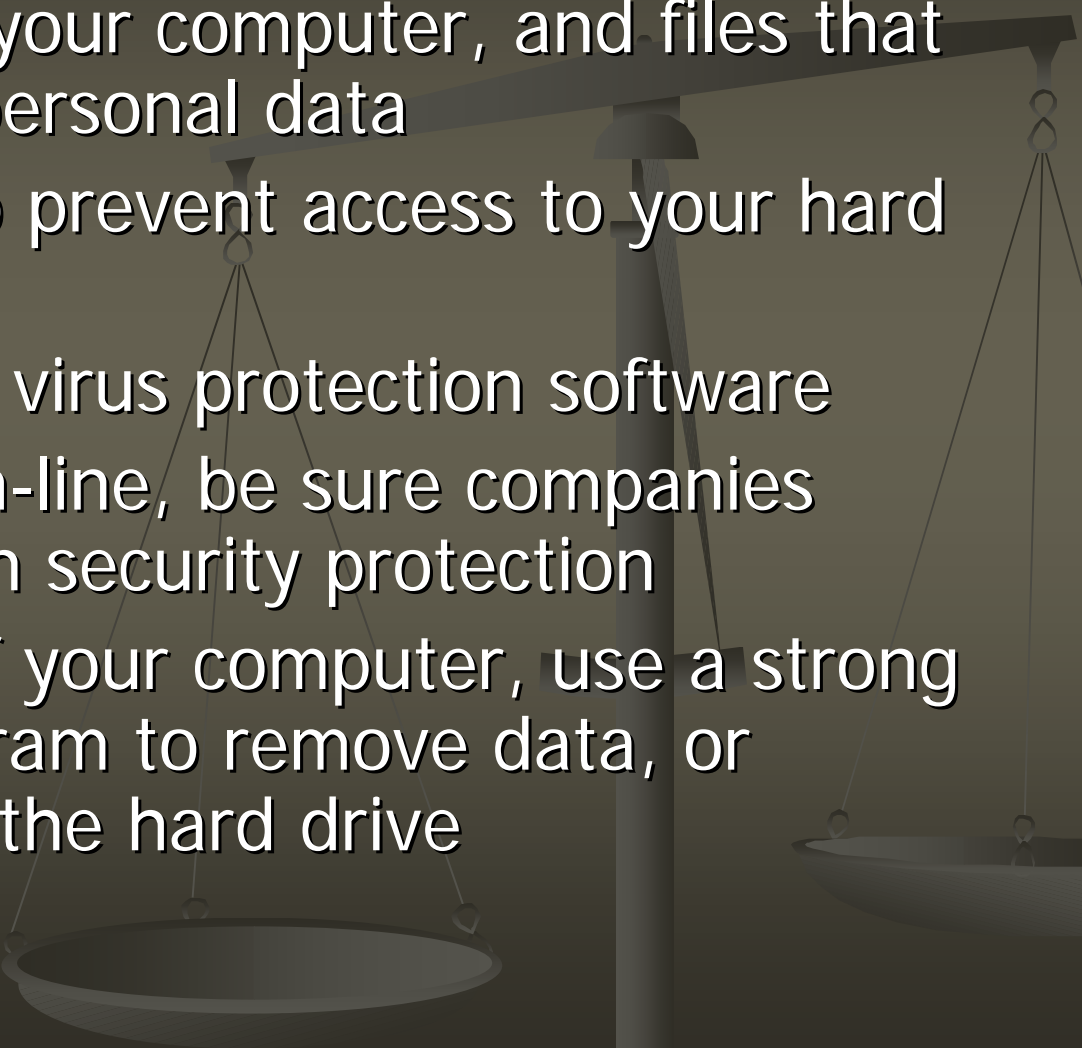
- Check your credit reports at least once a year
- Follow up if bills don't arrive on time
- Purchase a shredder
- Use a secured mailbox
- Do not print your SSN on checks
- Do not carry your SSN in your wallet/purse
- Keep items that contain your personal information in a safe place



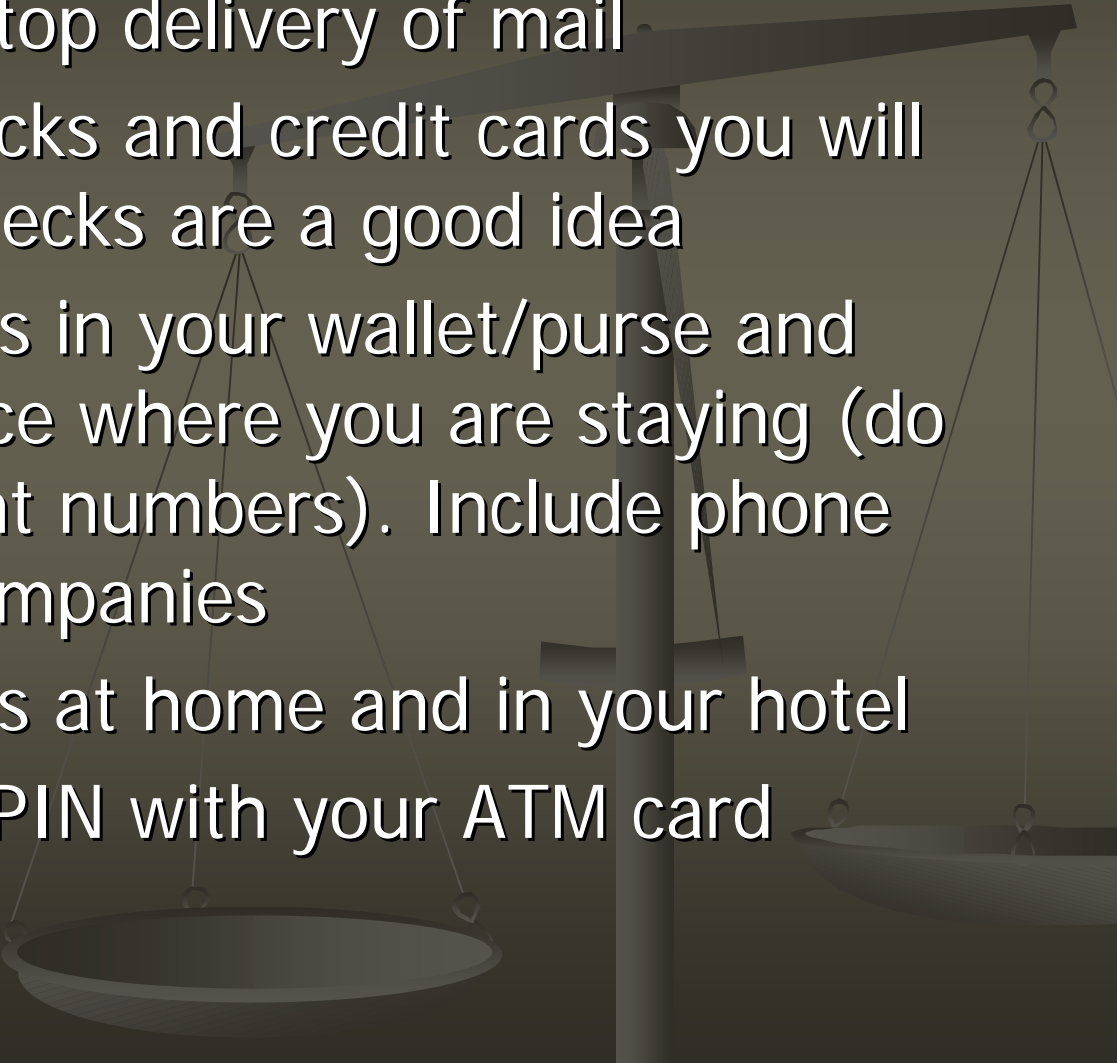
Other Prevention Tips

- Carry only the credit/debit cards you need when shopping
- Remove your name from the marketing lists of the three credit reporting bureaus
- Sign up for the Do-Not-Call registry
- Opt out of sharing your financial information when given the opportunity
- When ordering new checks, pick them up at the bank
- Never toss credit card receipts in a public trash container
- When creating passwords and PINs, use a combination of letters and numbers – memorize them!
- Shield your hand when using a bank ATM or making long-distance phone calls with your phone card

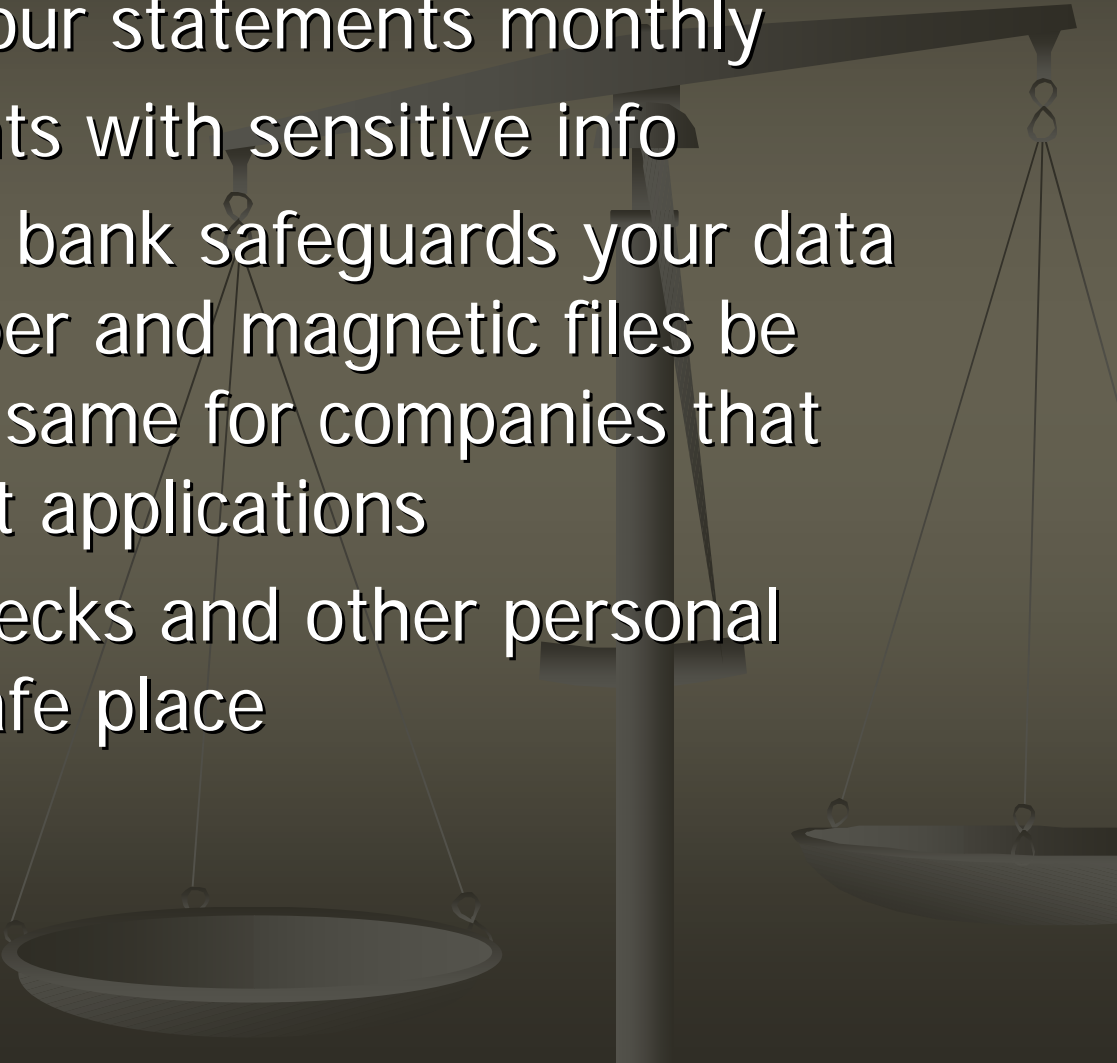
Prevention for Computer Users

- Password-protect your computer, and files that contain sensitive personal data
 - Install a firewall to prevent access to your hard drive by thieves
 - Install and update virus protection software
 - When shopping on-line, be sure companies provide transaction security protection
 - When disposing of your computer, use a strong “wipe” utility program to remove data, or physically destroy the hard drive
- 

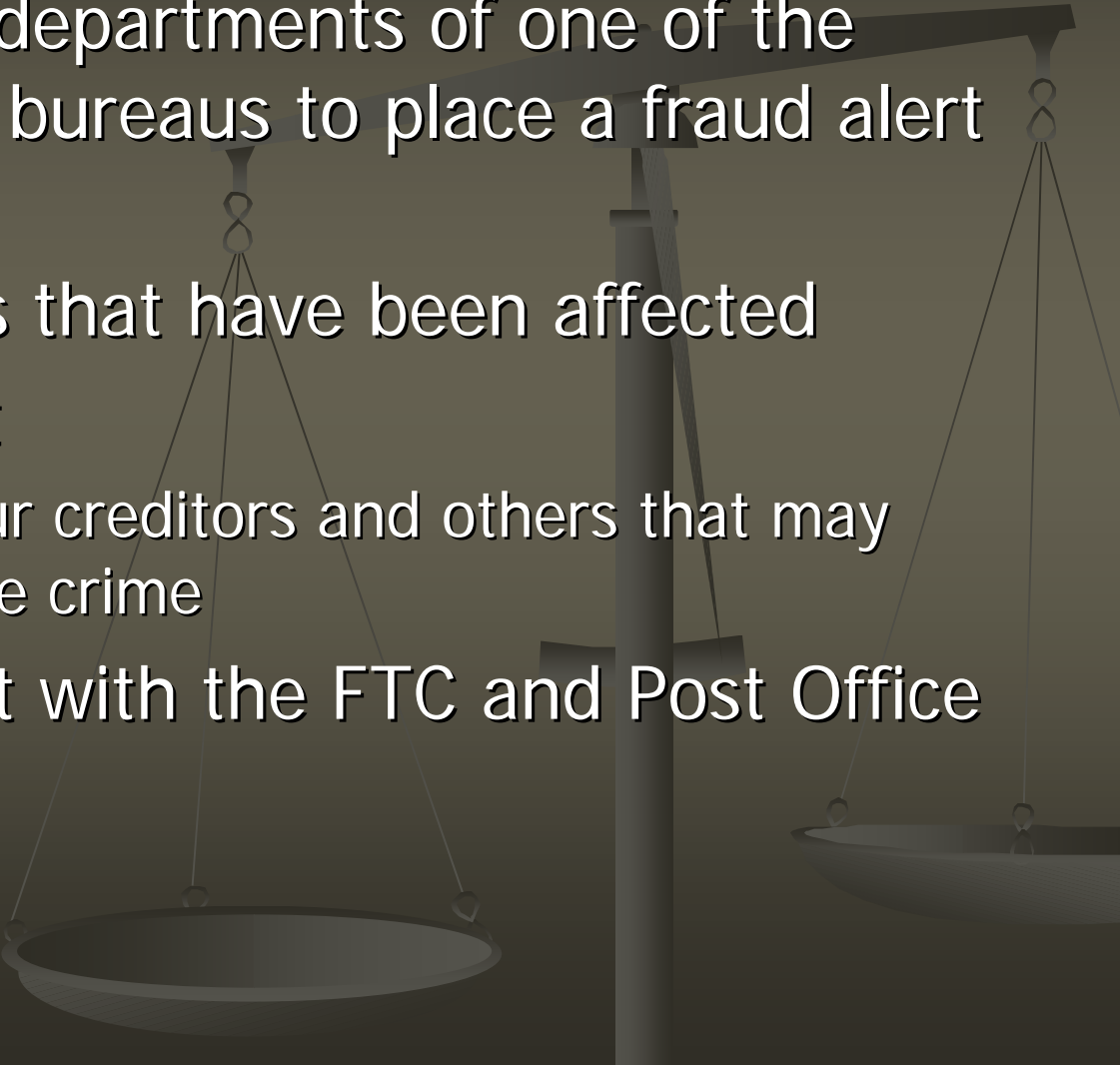
Protection When Traveling

- Have Post Office stop delivery of mail
 - Carry only the checks and credit cards you will need. Travelers checks are a good idea
 - Make a list of items in your wallet/purse and store in a safe place where you are staying (do not include account numbers). Include phone numbers of the companies
 - Lock up documents at home and in your hotel
 - Do not keep your PIN with your ATM card
- 

Handling Information Responsibly

- Carefully review your statements monthly
 - Shred all documents with sensitive info
 - Find out how your bank safeguards your data and insist that paper and magnetic files be destroyed. Do the same for companies that issue loan or credit applications
 - Store cancelled checks and other personal information in a safe place
- 

What To Do If You're a Victim

- Contact the fraud departments of one of the three major credit bureaus to place a fraud alert on your credit file
 - Close the accounts that have been affected
 - File a police report
 - Send copies to your creditors and others that may require proof of the crime
 - File your complaint with the FTC and Post Office
- 

Identity Theft Contacts

- Contact the Identity Theft Resource Center at:
 - 858-693-7935, or
 - www.idtheftcenter.org
- Contact Federal Trade Commission at:
 - 800-IDTHEFT, or
 - www.consumer.gov/idtheft
- Contact Fraud Units of Credit Reporting Bureaus at:
 - EQUIFAX: 800-525-6285
 - EXPERIAN: 888-397-3742
 - TRANS UNION: 800-680-7289
- For fraudulent use of checks, contact:
 - Checkwrite: 800-766-2748
 - Chexsystems: 800-428-9623
 - Equifax Telecredit: 800-437-5120
 - National Processing Co.: 800-526-5380
 - **SCAN: 800-262-7771**



Identity Theft Procedures

1. Buy a notebook to serve as a telephone log and file folders to keep notes on each contact;
2. File a police report in each jurisdiction where the theft occurred;
3. Close all accounts. Phone each company's fraud division. Request copy of relevant fraud-dispute form. Complete and return immediately;
4. Request a new driver's license from the state motor vehicle agency and have a fraud report attached to your driving record;
5. Send certified, return receipt requested letter to each person contacted, summarizing each conversation;
6. Notify check-verification firms about any fraudulent checks (Int'l. Check Service @ 800-526-5380; Telecheck @ 800-927-0755; Certery Check Services @ 800-437-5120);
7. Order credit reports from: www.annualcreditreport.com, or 1-877-322-8228. To do so in writing, get an Annual Credit Report Request Form from ftc.gov/credit, fill it out and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281
8. Have fraud alerts placed on all accounts and make sure new ones are not opened unless you are notified;
9. Refuse to pay fraudulent charges. Documenting the above helps;
10. Contact the Identity Theft Resource Center @ 858-693-7935 or at www.idtheftcenter.org for more tips.

Do-Not-Call Registry

- FTC's Do Not Call Registry launched
 - Register at www.donotcall.gov now, or call 888-382-1222 (call from the number you want to register)
 - Impacts interstate calls only
 - Enforcement began Oct. 1, 2003 or 3 months after you register
 - Won't stop political, charitable and survey calls
 - Violators can be fined up to \$11,000 per call
 - Call 1-888-CALL-FCC and file a complaint

Limiting Access



- FTC's Do Not Call Registry
 - Register at:
 - www.donotcall.gov, or
 - 888-382-1222
 - File a complaint at:
 - 888-CALL-FCC
- To Stop Credit Card Offers
 - 888-5-OPT-OUT
- Write to firms you do business with that you do not want info about you sold to others

Limiting Access

- To remove your name from national mailing lists, www.the-dma.org, or write to:
 - Mail Preference Service
P.O. Box 643
Carmel, NY 10512
- For problems with a mail order company, write to:
 - Mail Order Action Line
1111 19th Street, N.W., Suite 1100
Washington, DC 20036